

WHAT IS CLAIMED IS:

1. A power-residue calculating unit comprising:
 - a first register group holding a first kind of data;
 - a second register group holding a kind of data to be referred to concurrently with the data held in said first register group;
 - 5 a first internal bus connected to said first register group;
 - a second internal bus connected to said second register group;
 - a Montgomery multiplication residue calculation executing portion connected to said first and second internal buses for concurrently referring to values held in said first and second register groups and executing a
 - 10 Montgomery multiplication residue calculation;
 - a power-residue calculation executing portion connected to said first and second internal buses and said Montgomery multiplication residue calculation executing portion for concurrently referring to values held in said first and second register groups, communicating data with said
 - 15 Montgomery multiplication residue calculation executing portion, and executing a power-residue calculation; and
 - a pseudo calculation executing portion for executing in a pseudo manner an intermediate calculation process that can be omitted to obtain each calculation result of said Montgomery multiplication residue
 - 20 calculation and said power-residue calculation.

2. The power-residue calculating unit according to claim 1 wherein said pseudo calculation executing portion includes a dummy register connected to said first internal bus for once storing an intermediate calculation result to be discarded when said power-residue calculation is
- 5 executed in accordance with a binary method.

3. The power-residue calculating unit according to claim 1 wherein said first register group includes an intermediate result storing register for storing an intermediate result of said power-residue calculation when said power-residue calculation is executed in accordance with a binary

5 method, and

said pseudo calculation executing portion includes a replacing portion replacing said intermediate result at a time when 1 first appears starting from a most significant bit of a binary integer bit value representative of a power, with a value of a number to be raised to said power, rather than setting an initial value of said intermediate result storing register as a unit element.

4. The power-residue calculating unit according to claim 3 wherein said replacing portion replaces said intermediate result with a value of a number to be raised to said power by storing an operand changed to a sum of 0 and said number to be raised into said intermediate result storing register, in a calculation of said intermediate result to be stored in said intermediate result storing register, in a correction calculation of said Montgomery multiplication residue.

5. The power-residue calculating unit according to claim 1 wherein said second register group includes an accumulative addition register storing a value in the middle of an iterative accumulative addition, and

5 said pseudo calculation executing portion includes a reading portion reading a value 0 as a value in said accumulative addition register in place of a value in said accumulative addition register when 1 first appears starting from a least significant bit of each bit value of a multiplier, rather than setting an initial value in said accumulative addition register as an additive identity.

6. The power-residue calculating unit according to claim 1 wherein said second register group includes an accumulative addition register storing a value in the middle of an iterative accumulative addition in said Montgomery multiplication residue calculation,

5 said Montgomery multiplication residue calculation executing portion includes an accumulative adder for use in common with both said

Montgomery multiplication residue calculation and a correction calculation for said Montgomery multiplication residue calculation, and

10 said pseudo calculation executing portion includes a register input/output portion for performing a write operation for said accumulative addition register independently of whether said correction calculation is required or not.

7. The power-residue calculating unit according to claim 6 wherein said register input/output portion includes

5 a right shift portion performing right shift processing on a result of said correction calculation for writing into said accumulative addition register,

 a temporary holding register for holding a least significant bit of a result of said correction calculation in said right shift processing, and

10 a left shift portion left-shifting a read value from said accumulative addition register and adding a value stored in said temporary holding register to a left-shift result as a least significant bit.

8. The power-residue calculating unit according to claim 1 wherein said second register group includes

5 an accumulative addition register storing a value in the middle of an iterative accumulative addition in said Montgomery multiplication residue calculation and

 a dummy register,

10 said Montgomery multiplication residue calculation executing portion includes an accumulative adder for use in common with both said Montgomery multiplication residue calculation and a correction calculation in said Montgomery multiplication residue calculation, and

15 said pseudo calculation executing portion includes a register input/output portion performing a write operation for said accumulative addition register when said correction calculation is required, and performing a write operation for said dummy register when said correction calculation is not required.

9. The power-residue calculating unit according to claim 1 further comprising a dummy register for providing an input of a calculation when an intermediate calculation result to be discarded is calculated, and once storing said intermediate calculation result to be discarded.